Claims

What is claimed is:

1. A method to improve security in a wireless network, the method comprising:

determining a time period, the time period indicating when at least one new key is to be generated;

loading a number of keys in a controller, the number set so that a device connected to the wireless network can miss being re-authenticated for a predetermined number of the time periods and still communicate in a secure manner on the wireless network; and

communicating the keys from the controller to the device.

2. The method of claim 1, wherein the time period further indicates when devices communicating with the wireless network are to be re-authenticated.

3. The method of claim 1, wherein the step of determining a time period, the time period indicating when at least one new key is to be generated; further comprises the step of loading the time period in the controller.

4. The method of claim 1, wherein:

the method further comprises the step of selecting one of the keys as a local transmit key; and

the step of communicating the keys to a device further comprises the step of communicating to the device that a particular key of the keys is to be a transmit key for the device, wherein the particular key is selected to be different from the local transmit key.

5. The method of claim 4, wherein:

the controller is operating in a mixed mode;

the step of loading a plurality of keys comprises the steps of:

loading a fixed key; and

loading at least one additional key, wherein the number of keys comprises the fixed key and the at least one additional key; and

the step of selecting one of the keys as a local transmit key comprises the step of selecting the fixed key as the local transmit key.

6. The method of claim 5, wherein the at least one additional key is one key and the predetermined number of time periods is one.

7. The method of claim 1, wherein:

the controller is operating in a standard mode;

the step of loading a number of keys comprises loading at least three keys;

the method further comprises the steps of:

selecting one of the keys as a local transmit key; and

selecting the other keys as local receive keys; and

the step of communicating the keys comprises communicating the at least the three keys to the device.

8. The method of claim 7, wherein the at least three keys are three keys and wherein the predetermine number of the time periods is one.

9. The method of claim 1, wherein the method further comprises the steps of:

determining, every time period, at least one new key; and

replacing one of the keys with the at least one new key when the plurality of keys reaches a predetermined number of keys, else adding the at least one new key to the plurality of keys.

10. The method of claim 1, wherein:

the method further comprises the step of, for each time period, selecting one of the keys as a local transmit key, wherein the local transmit key for a current period is selected to be different than the local transmit key for an immediately preceding time period.

11. A method to improve security in a wireless network, the method comprising:

loading a time period, the time period indicating when at least one new key is to be generated;

loading a plurality of keys;

selecting one of the keys as a local transmit key;

selecting the other keys as receive keys;

performing the following steps every time period:

(i) generating at least one new key;

(ii) using the at least one new key to replace, for each of the at least one keys, one key of the plurality of keys, the at least one new key and any keys not replaced comprising a new plurality of keys; and

(iii) selecting a key of the new plurality of keys as a local transmit key, the local transmit key for a current time period selected to be different than the local transmit key for an immediately proceeding time period.

12. An apparatus for controlling access to a wireless network, the apparatus comprising:

a memory that stores computer-readable code; and

a processor operatively coupled to the memory, said processor configured to implement the computer-readable code, said computer-readable code configured to:

determine a time period, the time period indicating when at least one new key is to be generated;

load a number of keys, the number set so that a device connected to the wireless network can miss being re-authenticated for a predetermined number of the time periods and still communicate in a secure manner on the wireless network; and

communicate the keys from the controller to the device.

13. An article of manufacture comprising:

a computer readable medium having computer readable code means embodied thereon, said computer readable program code means comprising:

a step to determine a time period, the time period indicating when at least one new key is to be generated;

a step to load a number of keys, the number set so that a device connected to the wireless network can miss being re-authenticated for a predetermined number of the time periods and still communicate in a secure manner on the wireless network; and

a step to communicate the keys from the controller to the device.

14. A method performed on a device communicating with a wireless network, the method comprising:

loading a number of keys in the device, the number set so that the device can miss being re-authenticated for a predetermined number of time periods and still communicate on the wireless network;

using at least one key of the keys as a transmit key; and

using at least one key of the keys as receive keys.